CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being submitted *via* the USPTO EFS Filing System on the date shown below to **Mail Stop Appeal Brief - Patents**, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: August 1, 2008 /Jessica Sexton/
Jessica Sexton

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:			
Appellant(s):	Andrew Ritz, *et al.*	Examiner:	Chun Kuan Lee
Serial No:	10/777,368	Art Unit:	2181
Filing Date:	February 12, 2004		

Title: SYSTEM AND METHOD FOR DETECTING DMA-GENERATED MEMORY CORRUPTION IN A PCI EXPRESS BUS SYSTEM

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

Appellants' representative submits this brief in connection with an appeal of the above-identified patent application. Payment via credit card is submitted herewith in connection with all fees due regarding this appeal brief. In the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [MSFTP553US].

I. Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in the present appeal is Microsoft Corporation, the assignee of the present application.

II. Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))

Appellants, appellants' legal representative, and/or the assignee of the present application are not aware of any appeals or interferences which may be related to, will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

Claims 1-5, 7-17 and 19-22 stand rejected by the Examiner. The rejection of claims 1-5, 7-17 and 19-22 is being appealed. Claims 6 and 18 have been cancelled.

IV. Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))

No claims were amended subsequent to the Final Office Action dated April 3, 2008.

V. Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))

A. Independent Claim 1

Independent claim 1 recites a direct memory access memory corruption detection system embodied on a computer readable medium comprising the following computer executable components:

an access data store that stores access information associated with memory, the access data store comprising an access table, the access table comprising a source identifier field, a memory address field and an access attribute field, the access attribute field distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory address range associated with the access attribute identified in the source identifier field and memory address field; and, (*See e.g.*, page 7, lines 6-9; page 8, lines 8-22)

a memory controller that employs the access information to determine whether a requested direct memory access is permitted and rejects the requested direct memory access if it

is not permitted and allows the requested direct memory access if it is permitted. (*See e.g.*, page 7, lines 9-11; page 8, lines 23-31)

B. Independent Claim 14

Independent claim 14 recites a direct memory access memory corruption detection system embodied on a computer readable medium comprising the following computer executable components:

a memory controller that includes an access data store comprising an access table, the access table comprising a source identifier field, a memory address field and an access attribute field, the access attribute field contains an access attribute that distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory address range associated with the access attribute identified in the source identifier field and memory address field, wherein the access attribute contains data indicating read when the source identified by the source identifier associated with the access attribute is only permitted to read the memory address range associated with the access attribute, wherein the access attribute contains data indicating write when the source identified by the source identifier associated with the access attribute is only permitted to write to the memory address range associated with the access attribute, wherein the access attribute contains data indicating read and write when the source identified by the source identifier associated with the access attribute is permitted to read and write to the memory address range associated with the access attribute, wherein the access attribute contains data indicating no access when the source identified by the source identifier associated with the access attribute is not permitted access to the memory address range associated with the access attribute, the memory controller employs the access information to determine whether a requested direct memory access is permitted and rejects the requested direct memory access if it is not permitted and allows the requested direct memory access if it is permitted; and, (*See e.g.*, page 7, lines 6-11; page 8, lines 8-31)

a device driver that programs a device for a direct memory access operation, and, provides the access information to the memory controller *via* a direct memory access application interface. (*See e.g.*, page 9, line 29 to page 10, line 1)

C. Independent Claim 17

Independent claim 17 recites a method that facilitates detection of direct memory access memory corruption comprising:

receiving a request for a direct memory access transaction, the request comprising a source identifier, at least one memory address, and an access attribute; and, (*See e.g.*, page 11, lines 28-30)

determining whether the request is permitted based, at least in part on, stored access information and the request, the stored access information comprising at least one source identifier, at least one memory address range and at least one access attribute, an access attribute distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory range associated with the access attribute identified by the at least one source identifier and at least one memory address range; and (*See e.g.*, page 7, lines 6-9; page 8, lines 8-22; page 11, line 30 to page 12, line 6)

rejecting the requested direct memory access if it is not permitted and allowing the direct memory access if it is permitted. (*See e.g.*, page 12, lines 6-8)

D. Independent Claim 21

Independent claim 21 recites a data packet transmitted between two or more components embodied on a computer readable medium that facilitates detection of direct memory access memory corruption, the data packet comprising:

a data field comprising a corrected platform error event, the corrected platform error event being based, at least in part, upon a determination that a requested direct memory access is not permitted, the determination being based, at least in part, upon access information stored in an access table and the requested direct memory access, the access information comprising at least one source identifier, at least one memory address range and at least one access attribute, the at least one access attribute distinguishes from amongst read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source and memory address range identified by the at least one source identifier and at least one memory address range associated with the at least one access attribute. (*See e.g.*, page 6, lines 5-6; page 7, lines 6-11; page 8, lines 8-31; page 10, lines 13-15)

E. Independent Claim 22

Independent claim 22 recites a direct memory access memory corruption detection system embodied on a computer readable medium comprising:

means for storing access information associated with memory; (*See e.g.*, page 7, lines 6-9; page 8, lines 8-22)

means for receiving a request for a direct memory access; (*See e.g.*, page 7, line 20 to page 8, line 6)

means for determining whether a requested direct memory access is permitted based, at least in part, upon the stored access information and the request, the stored access information comprising at least one source identifier, at least one memory address range and at least one access attribute, the at least one access attribute distinguishes between read, read and write, write, and no access to indicate one of read, read and write, write, or no access for a combination of source and memory address range identified by the at least one source identifier and at least one memory address range associated with the at least one access attribute; and,

means for rejecting the requested direct memory access if it is not permitted and allowing the direct memory access if it is permitted. *See e.g.*, page 7, lines 6-11; page 8, lines 8-31)

VI. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A. Whether claims 1-5 and 7-13 are unpatentable under 35 U.S.C. §103(a) over Safranek *et al.* (US 2004/0193755) in view of Kondratiev *et al.* (US 6,922,740).

B. Whether claims 14-16 are unpatentable under 35 U.S.C. §103(a) over Safranek *et al.* (US 2004/0193755) in view of Kondratiev *et al.* (US 6,922,740).

C. Whether claims 17, 19, and 20 are unpatentable under 35 U.S.C. §103(a) over Safranek *et al.* (US 2004/0193755) in view of Kondratiev *et al.* (US 6,922,740).

D. Whether claim 21 is unpatentable under 35 U.S.C. §103(a) over Safranek *et al.* (US 2004/0193755) in view of Kondratiev *et al.* (US 6,922,740).

E. Whether claim 22 is unpatentable under 35 U.S.C. §103(a) over Safranek *et al.* (US 2004/0193755) in view of Kondratiev *et al.* (US 6,922,740).

VII. Argument (37 C.F.R. §41.37(c)(1)(vii))

A. Rejection of Claims 1-5 and 7-13 Under 35 U.S.C §103(a)

Claims 1-5 and 7-13 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Safranek et al. (US 2004/0193755) in view of Kondratiev et al. (US 6,922,740). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Sanfranek *et al.* and Kondratiev *et al.*, alone or in combination, do not teach each and every element of appellants' invention as recited in the subject claims.

> A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning. See *KSR v. Teleflex*, 550 U.S. ___, 127 S. Ct. 1727 (2007) citing Graham v. John Deere Co. of Kansas City, 383 U. S. 1, 36 (warning against a "temptation to read into the prior art the teachings of the invention in issue" and instructing courts to "'guard against slipping into the use of hindsight'" (*quoting Monroe Auto Equipment Co. v. Heckethorn Mfg. & Supply Co.*, 332 F. 2d 406, 412 (CA6 1964))).

Independent claim 1 recites *an access data store that stores access information associated with memory, the access data store comprising an access table,* ***the access table comprising a source identifier field, a memory address field and an access attribute field, the access attribute field distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory address range associated with the access attribute identified in the source identifier field and memory address field****; and a memory controller that employs the access information to determine whether a requested direct memory access is permitted and rejects the requested direct memory access if it is not permitted.*

As conceded in the Office Action, Sanfranek *et al.* does not teach or suggest the aforementioned novel aspects of appellant's invention as recited in the subject claims. The cited art discloses a method for preventing non-CPU devices from accessing protected memory. This is accomplished by maintaining a NODMA memory cache where each bit in the cache represents a page of memory. The setting of the bit (0 or 1) determines if the associated memory page is protected. If a memory access request for a page comes from a non-CPU device and the NODMA cache indicates that the page is protected, the access will be denied. However, this

provides very fine control of memory pages, but lacks the combined source, memory, and access type control of the subject claim. Kondratiev *et al.* is cited to make up for the above noted deficiencies of Sanfranek *et al.*, but also fails to teach all novel features of the subject claim. Kondratiev *et al.* teaches a system for controlling DMA access from devices. The Office Action cites Figure 2 and column 4, lines 40-65 as teaching the *source identifier field, memory address field and access attribute field* of the subject claim. However, the cited art discloses a table that contains rows containing device ID field, read memory range field, write memory range field and duration field. This provides an access control list that indicates memory ranges a device is allowed to access. The table *only* indicates memory ranges that are allowed access. It does not provide the ability to directly specify a memory range that is not allowed access. Moreover, read and write access are indicated in two separate fields by specifying a memory address range in each of the two separate read memory range and write memory range fields. This table of the cited reference fails to teach an access attribute field as recited in the subject claim. The access attribute in appellant's claimed invention provides within a single field an indication distinguishing between both allowed and disallowed access information including access type. This provides allowed and disallowed control information to be stored together, as well as providing both types of information for a single device. For example, the table can have an entry for device A indicating read access for memory range X and another entry for device A indicating no access for memory range Z. In another example, the table could have an entry for device B indicating no access for memory range Y, thereby allowing it access to all memory ranges except Y. Using the combination of a source identifier field, a memory address field and an access attribute field to define allowed and disallowed access provides for more robust and efficient definition of memory access privileges using reduced table space. As recited in the subject claim, the access attribute has specific indicators for each of read, write, read and write, and no access for a specified source and memory range. Sanfranek *et al.* and Kondratiev *et al.* fail to disclose this novel feature recited in the subject claim.

Accordingly, appellants' representative respectfully submits that Sanfranek *et al.* and Kondratiev *et al.*, alone or in combination, fail to teach or suggest all limitations as recited in independent claim 1 (and claims 2-5 and 7-13 that depend there from) and thus fails to make obvious the subject claimed invention. For this reason, this rejection should be withdrawn.

B. Rejection of Claims 14-16 Under 35 U.S.C §103(a)

Claims 14-16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Safranek et al. (US 2004/0193755) in view of Kondratiev et al. (US 6,922,740). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Sanfranek *et al.* and Kondratiev *et al.*, alone or in combination, do not teach each and every element of appellants' invention as recited in the subject claims.

Independent claim 14 recites *a memory controller that includes an access data store comprising an access table,* ***the access table comprising a source identifier field, a memory address field and an access attribute field****, the access attribute field contains an access attribute that distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory address range associated with the access attribute identified in the source identifier field and memory address field,* ***an access attribute distinguishes from amongst read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source and memory address range identified by a source identifier associated with the access attribute and a memory address range associated with the access attribute, wherein the access attribute contains data indicating read when the source identified by the source identifier associated with the access attribute is only permitted to read the memory address range associated with the access attribute, wherein the access attribute contains data indicating write when the source identified by the source identifier associated with the access attribute is only permitted to write to the memory address range associated with the access attribute, wherein the access attribute contains data indicating read and write when the source identified by the source identifier associated with the access attribute is permitted to read and write to the memory address range associated with the access attribute, wherein the access attribute contains data indicating no access when the source identified by the source identifier associated with the access attribute is not permitted access to the memory address range associated with the access attribute****, the memory controller employs the access information to determine whether a requested direct memory access is permitted and rejects the requested direct memory access if it is not permitted and allows the requested direct memory access if it is permitted.*

As conceded in the Office Action, Sanfranek *et al.* does not teach or suggest the aforementioned novel aspects of appellant's invention as recited in the subject claims. The cited art discloses a method for preventing non-CPU devices from accessing protected memory. This is accomplished by maintaining a NODMA memory cache where each bit in the cache represents a page of memory. The setting of the bit (0 or 1) determines if the associated memory page is protected. If a memory access request for a page comes from a non-CPU device and the NODMA cache indicates that the page is protected, the access will be denied. However, this provides very fine control of memory pages, but lacks the combined source, memory, and access type control of the subject claim. Kondratiev *et al.* is cited to make up for the above noted deficiencies of Sanfranek *et al.*, but also fails to teach all novel features of the subject claim. Kondratiev *et al.* teaches a system for controlling DMA access from devices. The Office Action cites Figure 2 and column 4, lines 40-65 as teaching the *source identifier field, memory address field and access attribute field* of the subject claim. However, the cited art discloses a table that contains rows containing device ID field, read memory range field, write memory range field and duration field. This provides an access control list that indicates memory ranges a device is allowed to access. The table *only* indicates memory ranges that are allowed access. It does not provide the ability to directly specify a memory range that is not allowed access. Moreover, read and write access are indicated in two separate fields by specifying a memory address range in each of the two separate read memory range and write memory range fields. This table of the cited reference fails to teach an access attribute field as recited in the subject claim. The access attribute in appellant's claimed invention provides within a single field an indication distinguishing between both allowed and disallowed access information including access type. This provides allowed and disallowed control information to be stored together, as well as providing both types of information for a single device. For example, the table can have an entry for device A indicating read access for memory range X and another entry for device A indicating no access for memory range Z. In another example, the table could have an entry for device B indicating no access for memory range Y, thereby allowing it access to all memory ranges except Y. Using the combination of a source identifier field, a memory address field and an access attribute field to define allowed and disallowed access provides for more robust and efficient definition of memory access privileges using reduced table space. Sanfranek *et al.* and Kondratiev *et al.* fail to disclose this novel feature discloses in the subject claim. The references

take a more data intensive approach by either mapping the entire memory space to bit references or requiring separate fields for read and write access. These approaches provide less control for memory access and require more data table space. As recited in the subject claim, the access attribute has specific indicators for each of read, write, read and write, and no access for a specified source and memory range. The cited references do no teach all of the elements of claim 14.

Accordingly, appellants' representative respectfully submits that Sanfranek *et al.* and Kondratiev *et al.*, alone or in combination, fail to teach or suggest all limitations in independent claim 14 (and claim 15 and 16 that depend there from) and thus fails to make obvious the subject claimed invention. For this reason, this rejection should be withdrawn.

C. Rejection of Claims 17, 19 and 20 Under 35 U.S.C §103(a)

Claims 17, 19, and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Safranek et al. (US 2004/0193755) in view of Kondratiev et al. (US 6,922,740). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Sanfranek *et al.* and Kondratiev *et al.*, alone or in combination, do not teach each and every element of appellants' invention as recited in the subject claims.

Independent 17 recites *receiving a request for a direct memory access transaction, the request comprising a source identifier, at least one memory address, and an* ***access attribute****; and, determining whether the request is permitted based, at least in part on, stored access information and the request, the stored access information comprising at least one source identifier, at least one memory address range and at least one access attribute****, an access attribute distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory range associated with the access attribute identified by the at least one source identifier and at least one memory address range****.*

As conceded in the Office Action, Sanfranek *et al.* does not teach or suggest the aforementioned novel aspects of appellant's invention as recited in the subject claims. The cited art discloses a method for preventing non-CPU devices from accessing protected memory. This is accomplished by maintaining a NODMA memory cache where each bit in the cache represents a page of memory. The setting of the bit (0 or 1) determines if the associated memory page is

protected. If a memory access request for a page comes from a non-CPU device and the NODMA cache indicates that the page is protected, the access will be denied. However, this provides very fine control of memory pages, but lacks the combined source, memory, and access type control of the subject claim. Kondratiev *et al.* is cited to make up for the above noted deficiencies of Sanfranek *et al.*, but also fails to teach all novel features of the subject claim. Kondratiev *et al.* teaches a system for controlling DMA access from devices. The Office Action cites Figure 2 and column 4, lines 40-65 as teaching the *source identifier field, memory address field and access attribute field* of the subject claim. However, the cited art discloses a table that contains rows containing device ID field, read memory range field, write memory range field and duration field. This provides an access control list that indicates memory ranges a device is allowed to access. The table *only* indicates memory ranges that are allowed access. It does not provide the ability to directly specify a memory range that is not allowed access. Moreover, read and write access are indicated in two separate fields by specifying a memory address range in each of the two separate read memory range and write memory range fields. This table of the cited reference fails to teach an access attribute field as recited in the subject claim. The access attribute in appellant's claimed invention provides within a single field an indication distinguishing between both allowed and disallowed access information including access type. This provides allowed and disallowed control information to be stored together, as well as providing both types of information for a single device. For example, the table can have an entry for device A indicating read access for memory range X and another entry for device A indicating no access for memory range Z. In another example, the table could have an entry for device B indicating no access for memory range Y, thereby allowing it access to all memory ranges except Y. Using the combination of a source identifier field, a memory address field and an access attribute field to define allowed and disallowed access provides for more robust and efficient definition of memory access privileges using reduced table space. As recited in the subject claim, the access attribute has specific indicators for each of read, write, read and write, and no access for a specified source and memory range. Sanfranek *et al.* and Kondratiev *et al.* fail to disclose this novel feature recited in the subject claim.

Accordingly, appellants' representative respectfully submits that Sanfranek *et al.* and Kondratiev *et al.*, alone or in combination, fail to teach or suggest all limitations as recited in

independent claim 17 (and claims 19 and 20 that depend there from) and thus fails to make obvious the subject claimed invention. For this reason, this rejection should be withdrawn.

D. Rejection of Claim 21 Under 35 U.S.C §103(a)

Claim 21 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Safranek et al. (US 2004/0193755) in view of Kondratiev et al. (US 6,922,740). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Sanfranek *et al.* and Kondratiev *et al.*, alone or in combination, do not teach each and every element of appellants' invention as recited in the subject claims.

Independent claim 21 recites *a data field comprising a corrected platform error event, the corrected platform error event being based, at least in part, upon a determination that a requested direct memory access is not permitted, the determination being based, at least in part, upon access information stored in an access table and the requested direct memory access, the access information comprising at least one source identifier, at least one memory address range and at least one access attribute,* ***the at least one access attribute distinguishes from amongst read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source and memory address range identified by the at least one source identifier and at least one memory address range associated with the at least one access attribute***.

As conceded in the Office Action, Sanfranek *et al.* does not teach or suggest the aforementioned novel aspects of appellant's invention as recited in the subject claims. The cited art discloses a method for preventing non-CPU devices from accessing protected memory. This is accomplished by maintaining a NODMA memory cache where each bit in the cache represents a page of memory. The setting of the bit (0 or 1) determines if the associated memory page is protected. If a memory access request for a page comes from a non-CPU device and the NODMA cache indicates that the page is protected, the access will be denied. However, this provides very fine control of memory pages, but lacks the combined source, memory, and access type control of the subject claim. Kondratiev *et al.* is cited to make up for the above noted deficiencies of Sanfranek *et al.*, but also fails to teach all novel features of the subject claim. Kondratiev *et al.* teaches a system for controlling DMA access from devices. The Office Action cites Figure 2 and column 4, lines 40-65 as teaching the *source identifier field, memory address*

field and access attribute field of the subject claim. However, the cited art discloses a table that contains rows containing device ID field, read memory range field, write memory range field and duration field. This provides an access control list that indicates memory ranges a device is allowed to access. The table *only* indicates memory ranges that are allowed access. It does not provide the ability to directly specify a memory range that is not allowed access. Moreover, read and write access are indicated in two separate fields by specifying a memory address range in each of the two separate read memory range and write memory range fields. This table of the cited reference fails to teach an access attribute field as recited in the subject claim. The access attribute in appellant's claimed invention provides within a single field an indication distinguishing between both allowed and disallowed access information including access type. This provides allowed and disallowed control information to be stored together, as well as providing both types of information for a single device. For example, the table can have an entry for device A indicating read access for memory range X and another entry for device A indicating no access for memory range Z. In another example, the table could have an entry for device B indicating no access for memory range Y, thereby allowing it access to all memory ranges except Y. Using the combination of a source identifier field, a memory address field and an access attribute field to define allowed and disallowed access provides for more robust and efficient definition of memory access privileges using reduced table space. As recited in the subject claim, the access attribute has specific indicators for each of read, write, read and write, and no access for a specified source and memory range. Sanfranek *et al.* and Kondratiev *et al.* fail to disclose this novel feature discloses in the subject claim.

Accordingly, appellants' representative respectfully submits that Sanfranek *et al.* and Kondratiev *et al.*, alone or in combination, fail to teach or suggest all limitations as recited in independent claim 21 and thus fails to make obvious the subject claimed invention. For this reason, this rejection should be withdrawn.

E. Rejection of Claim 22 Under 35 U.S.C §103(a)

Claim 22 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Safranek et al. (US 2004/0193755) in view of Kondratiev et al. (US 6,922,740). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Sanfranek *et al.* and

Kondratiev *et al.*, alone or in combination, do not teach each and every element of appellants' invention as recited in the subject claims.

Independent claim 22 recites *means for determining whether a requested direct memory access is permitted based, at least in part, upon the stored access information and the request, the stored access information comprising at least one source identifier, at least one memory address range and at least one access attribute,* ***the at least one access attribute distinguishes between read, read and write, write, and no access to indicate one of read, read and write, write, or no access for a combination of source and memory address range identified by the at least one source identifier and at least one memory address range associated with the at least one access attribute***.

As conceded in the Office Action, Sanfranek *et al.* does not teach or suggest the aforementioned novel aspects of appellant's invention as recited in the subject claims. The cited art discloses a method for preventing non-CPU devices from accessing protected memory. This is accomplished by maintaining a NODMA memory cache where each bit in the cache represents a page of memory. The setting of the bit (0 or 1) determines if the associated memory page is protected. If a memory access request for a page comes from a non-CPU device and the NODMA cache indicates that the page is protected, the access will be denied. However, this provides very fine control of memory pages, but lacks the combined source, memory, and access type control of the subject claim. Kondratiev *et al.* is cited to make up for the above noted deficiencies of Sanfranek *et al.*, but also fails to teach all novel features of the subject claim. Kondratiev *et al.* teaches a system for controlling DMA access from devices. The Office Action cites Figure 2 and column 4, lines 40-65 as teaching the *source identifier field, memory address field and access attribute field* of the subject claim. However, the cited art discloses a table that contains rows containing device ID field, read memory range field, write memory range field and duration field. This provides an access control list that indicates memory ranges a device is allowed to access. The table *only* indicates memory ranges that are allowed access. It does not provide the ability to directly specify a memory range that is not allowed access. Moreover, read and write access are indicated in two separate fields by specifying a memory address range in each of the two separate read memory range and write memory range fields. This table of the cited reference fails to teach an access attribute field as recited in the subject claim. The access attribute in appellant's claimed invention provides within a single field an indication

distinguishing between both allowed and disallowed access information including access type. This provides allowed and disallowed control information to be stored together, as well as providing both types of information for a single device. For example, the table can have an entry for device A indicating read access for memory range X and another entry for device A indicating no access for memory range Z. In another example, the table could have an entry for device B indicating no access for memory range Y, thereby allowing it access to all memory ranges except Y. Using the combination of a source identifier field, a memory address field and an access attribute field to define allowed and disallowed access provides for more robust and efficient definition of memory access privileges using reduced table space. As recited in the subject claim, the access attribute has specific indicators for each of read, write, read and write, and no access for a specified source and memory range. Sanfranek *et al.* and Kondratiev *et al.* fail to disclose this novel feature discloses in the subject claim.

Independent claim 22 recites *means for determining whether a requested direct memory access is permitted based, at least in part, upon the stored access information and the request, the stored access information comprising at least one source identifier, at least one memory address range and at least one access attribute,* ***the at least one access attribute distinguishes between read, read and write, write, and no access to indicate one of read, read and write, write, or no access for a combination of source and memory address range identified by the at least one source identifier and at least one memory address range associated with the at least one access attribute.*** Sanfranek *et al.* and Kondratiev *et al.*, alone or in combination, fail to teach or suggest an access attribute that can distinguish between all of read, write, read and write, and no access for a specified source and memory range. As such, the cited references fail to teach all novel aspects of the subject claim.

Accordingly, appellants' representative respectfully submits that Sanfranek *et al.* and Kondratiev *et al.*, alone or in combination, fail to teach or suggest all limitations as recited in independent claim 22 and thus fails to make obvious the subject claimed invention. For this reason, this rejection should be withdrawn.

F. Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejections of claims 1-5, 7-17 and 19-22 be reversed.

If any additional fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP553US].

Respectfully submitted,
AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24th Floor, National City Center
1900 East 9th Street
Cleveland, Ohio
Telephone: (216) 696-8730
Facsimile: (216) 696-8731

VIII. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1. A direct memory access memory corruption detection system embodied on a computer readable medium comprising the following computer executable components:

an access data store that stores access information associated with memory, the access data store comprising an access table, the access table comprising a source identifier field, a memory address field and an access attribute field, the access attribute field distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory address range associated with the access attribute identified in the source identifier field and memory address field; and,

a memory controller that employs the access information to determine whether a requested direct memory access is permitted and rejects the requested direct memory access if it is not permitted and allows the requested direct memory access if it is permitted.

2. The direct memory access memory corruption detection system of claim 1, the access information comprising a direct memory access request.

3. The direct memory access memory corruption detection system of claim 2, the direct memory access request comprising a transaction type.

4. The direct memory access memory corruption detection system of claim 1, the direct memory access request comprising a source identifier.

5. The direct memory access memory corruption detection system of claim 4, the source identifier being associated with a device.

6. (Cancelled).

7. The direct memory access memory corruption detection system of claim 1, the access information comprising at least one permitted memory address.

8. The direct memory access memory corruption detection system of claim 1, the access information comprising at least one disallowed memory address.

9. The direct memory access memory corruption detection system of claim 1, the request comprising a read action or a write action.

10. The direct memory access memory corruption detection system of claim 1, the request comprising a peripheral component interconnect express bus transaction.

11. The direct memory access memory corruption detection system of claim 1, the memory controller coupled to a device through a peripheral component interconnect express bus, the device providing the request.

12. The direct memory access memory corruption detection system of claim 1, the memory controller further providing error information, if the requested direct memory access is not permitted.

13. The direct memory access memory corruption detection system of claim 12, the error information comprising source information associated with the requested direct memory access.

14. A direct memory access memory corruption detection system embodied on a computer readable medium comprising the following computer executable components:

a memory controller that includes an access data store comprising an access table, the access table comprising a source identifier field, a memory address field and an access attribute field, the access attribute field contains an access attribute that distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory address range associated with the access attribute identified in the source identifier field and memory address field, wherein the access attribute contains data indicating read when the source identified by the source identifier associated with the access attribute is only permitted to read the memory address range associated with the access attribute, wherein the access attribute contains data

indicating write when the source identified by the source identifier associated with the access attribute is only permitted to write to the memory address range associated with the access attribute, wherein the access attribute contains data indicating read and write when the source identified by the source identifier associated with the access attribute is permitted to read and write to the memory address range associated with the access attribute, wherein the access attribute contains data indicating no access when the source identified by the source identifier associated with the access attribute is not permitted access to the memory address range associated with the access attribute, the memory controller employs the access information to determine whether a requested direct memory access is permitted and rejects the requested direct memory access if it is not permitted and allows the requested direct memory access if it is permitted; and,

a device driver that programs a device for a direct memory access operation, and, provides the access information to the memory controller *via* a direct memory access application interface.

15. The direct memory access memory corruption detection system of claim 14, the device driver providing access information comprising a range of physical memory, a source identifier, and, an access attribute.

16. The direct memory access memory corruption detection system of claim 14, the request comprising a peripheral component interconnect express bus transaction.

17. A method that facilitates detection of direct memory access memory corruption comprising:

receiving a request for a direct memory access transaction, the request comprising a source identifier, at least one memory address, and an access attribute; and,

determining whether the request is permitted based, at least in part on, stored access information and the request, the stored access information comprising at least one source identifier, at least one memory address range and at least one access attribute, an access attribute distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory

range associated with the access attribute identified by the at least one source identifier and at least one memory address range; and

rejecting the requested direct memory access if it is not permitted and allowing the direct memory access if it is permitted.

18. (Cancelled)

19. The method of claim 17, storing access information in a access data store, the access information comprising at least one source identifier, at least one memory address range and at least one an access attribute.

20. A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 17.

21. A data packet transmitted between two or more components embodied on a computer readable medium that facilitates detection of direct memory access memory corruption, the data packet comprising:

a data field comprising a corrected platform error event, the corrected platform error event being based, at least in part, upon a determination that a requested direct memory access is not permitted, the determination being based, at least in part, upon access information stored in an access table and the requested direct memory access, the access information comprising at least one source identifier, at least one memory address range and at least one access attribute, the at least one access attribute distinguishes from amongst read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source and memory address range identified by the at least one source identifier and at least one memory address range associated with the at least one access attribute.

22. A direct memory access memory corruption detection system embodied on a computer readable medium comprising:

means for storing access information associated with memory;

means for receiving a request for a direct memory access;

means for determining whether a requested direct memory access is permitted based, at least in part, upon the stored access information and the request, the stored access information comprising at least one source identifier, at least one memory address range and at least one access attribute, the at least one access attribute distinguishes between read, read and write, write, and no access to indicate one of read, read and write, write, or no access for a combination of source and memory address range identified by the at least one source identifier and at least one memory address range associated with the at least one access attribute; and,

means for rejecting the requested direct memory access if it is not permitted and allowing the direct memory access if it is permitted.

IX. Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

X. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.